

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

**CENTER FOR HEALTH INFORMATION & ANALYSIS
DATA USE AGREEMENT**

This Data Use Agreement (“Agreement”) is entered into between the Center for Health Information and Analysis (“CHIA”) and _____ (“Data Recipient”), effective as of the
[NAME OF ORGANIZATION]

date of execution below. The undersigned Data Recipient and all its authorized representatives, subcontractors, agents, and employees, in consideration for the receipt of All-Payer Claims Database data and/or Hospital Discharge Database data, and/or any data subsets derived therefrom (“CHIA Data”), agree that they will observe all of the conditions set forth below regarding the use of any CHIA Data that contain confidential data, personal data, and/or protected health information.

Data Recipient Obligations

- 1) The Data Recipient, its employees, agents, and/or contractors shall use CHIA Data ONLY for the specific purpose(s) stated in the Application submitted to CHIA pursuant to 957 CMR 5.00, as approved (with or without additional restrictions) by the Executive Director, and in accordance with the terms of this Agreement. The approved application, including any additional restrictions imposed by the Executive Director, is attached hereto as Exhibit A.
- 2) The Data Recipient, its employees, agents, and/or contractors shall follow all policies and procedures set forth in its Application, and shall use CHIA Data in conformity with each of the assurances made in the Application attached as Exhibit A.
- 3) The Data Recipient shall limit access to the CHIA Data to such authorized employees, agents, or contractors as are reasonably necessary to undertake the project approved by the Executive Director as described in Exhibit A.
- 4) All Data Recipient employees, agents, and contractors provided with access to CHIA Data shall sign the Confidentiality Agreement attached hereto as Exhibit B.
- 5) The Data Recipient shall provide CHIA with the names, contact information, and copies of the Confidentiality Agreements executed by any Data Recipient employees, agents, or contractors given access to CHIA Data.
- 6) The Data Recipient shall ensure that all employees, agents, and contractors with access to CHIA Data comply with the terms of this Agreement, as well as any applicable state and federal data privacy and security laws or regulations. The Data Recipient shall further ensure that all employees, agents, and contractors with access to CHIA Data put in place all appropriate administrative, technical, and physical safeguards to protect the privacy and security of CHIA Data in accordance with 45 CFR § 164.530(c). The Data Recipient shall ensure that all employees, agents, and contractors with access to CHIA Data meet the security standards, requirements, and implementation specifications as set forth in 45 CFR part 164, subpart C, Security Standards for the Protection of Electronic Protected Health Information.

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

- 7) CHIA Data may not be used for any purposes contrary to local, state, and federal laws and regulations. Compliance with all local, state, and federal laws and regulations is the sole responsibility of the Data Recipient.
- 8) The Data Recipient shall not publish or otherwise disclose any Restricted Use Data Elements, or any data derived or extracted from such data, in any paper, report, website, statistical tabulation, or similar document unless such paper, report, website, statistical tabulation, or similar document conforms to the standards for de-identification set forth under 45 CFR 165.514(a), (b)(2), and (c). The Data Recipient shall not publish or otherwise disclose in any public paper, report, website, statistical tabulation, or similar document any data on ten or fewer individuals or data derived from ten or fewer claims.
- 9) The Data Recipient agrees and acknowledges that because CHIA Data relies, in part, on the existence and proper operation of equipment and software that is outside of the control of CHIA, and relies on information controlled by and supplied by third parties, CHIA makes no representations, warranties, or guarantees as to the accuracy or completeness of any data.
- 10) The Data Recipient shall maintain or cause to be maintained sufficient insurance coverage as shall be necessary to insure the Data Recipient and its employees, agents, and subcontractors against any and all claims or claims for damages arising under this Agreement.
- 11) The Data Recipient agrees to defend, indemnify, and hold harmless CHIA from and against any and all claims, damages, losses, and liability, including reasonable attorney's fees, costs, expenses, fines, and penalties sustained or incurred by CHIA relating to or resulting from any action, failure, negligence, or willful acts or omissions of the Data Recipient's officers, employees, agents, third party contractors, or representatives, including failure to comply with any local, state, and/or federal laws and/or regulations. The Data Recipient agrees not to hold CHIA liable to the Data Recipient, or to any other party entitled to indemnification, for any consequential, indirect, special, exemplary, or punitive damages arising under or in connection with this Agreement or the use of CHIA Data. This includes any loss of profits, loss of revenue, loss of equipment use, or loss of data or information of any kind, even if such party has been advised of the possibility of such damages.
- 12) The applicant will cite the Center for Health Information and Analysis as the source of the data in any studies, reports, or products in which CHIA Data are used.

Data Recipient's Confidentiality and Security Obligations

- 1) The Data Recipient shall maintain such policies, procedures, and systems as may be reasonably necessary to prevent unauthorized parties from having access to, using, disclosing, processing, copying, modifying, corrupting, rendering unavailable, destroying, introducing computer code into, or otherwise performing activities or operations harmful to the privacy, availability, accessibility, integrity, structure, format, or content of CHIA Data that may be transmitted to or accessed by the Data Recipient.

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

- 2) The Data Recipient must assign a Project Manager, at a Director level or higher, to assume full responsibility for and compliance with the Data Recipient's data security standards and procedures.
- 3) All access to CHIA Data shall be logged by the Data Recipient and all such logs shall be made available to CHIA upon request.
- 4) The Data Recipient will implement the security measures described in "Safeguarding CHIA Data," attached hereto as Exhibit C.
- 5) The Data Recipient agrees to return or destroy any CHIA Data provided pursuant to this Data Use Agreement and to provide CHIA with an executed copy of Exhibit D, attesting to any such data destruction.
- 6) The Data Recipient agrees that it will permit CHIA, at its discretion, to audit the Data Recipient's compliance with this Data Use Agreement by providing CHIA with reasonable access to the Project Manager and documentation related to the access, use, and disclosure of CHIA data.
- 7) The Data Recipient agrees that it will permit CHIA to review all analyses, research, or other products created or based on CHIA Data prior to the release of or disclosure of any such analysis, research, or product.
- 8) CHIA's exercise or non-exercise of any authority under this Data Use Agreement to inspect the privacy or security practices of the Data Recipient shall not relieve the Data Recipient of any obligations set forth herein, nor be construed as a waiver of any of the Data Recipient's obligations or as an acceptance of any unsatisfactory practices or privacy or security failures or breaches by the Data Recipient.
- 9) The Data Recipient agrees that if it fails to comply with any of the requirements of this Data Use Agreement, or any applicable state or federal regulation or law, CHIA may deny future access to any CHIA Data, terminate current access to CHIA Data, and/or demand immediate return or destruction of all CHIA data.

Terms and Termination

1. The effective date of this Agreement shall be the date of execution below.
2. This Agreement shall be in effect until Data Recipient attests to the return or destruction of the CHIA Data provided pursuant to this Agreement.

Warranties; Limitations of Liability

CHIA MAKES NO REPRESENTATIONS OR WARRANTIES TO ANY PERSON OR ENTITY WITH RESPECT TO CHIA DATA, THE SOFTWARE, OR ANY OTHER INFORMATION PROVIDED BY CHIA OR ITS AGENTS WITH RESPECT TO ANY OF THE FOREGOING, AND HEREBY DISCLAIMS ALL IMPLIED WARRANTIES WITH RESPECT TO CHIA DATA, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

PARTICULAR PURPOSE. FURTHER, CHIA MAKES NO WARRANTY, GUARANTEE OR REPRESENTATION REGARDING THE USE, OR ANY INTENDED, EXPECTED, OR ACTUAL RESULTS OF THE USE, OF CHIA DATA, THE SOFTWARE, OR ANY OTHER INFORMATION PROVIDED BY CHIA IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. CHIA DOES NOT MAKE ANY WARRANTIES THAT CHIA DATA, SOFTWARE, OR ANY OTHER INFORMATION PROVIDED BY CHIA WILL BE ERROR-FREE. CHIA SPECIFICALLY DISCLAIMS ALL EXPRESS WARRANTIES NOT STATED HEREIN AND ALL IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO CHIA AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY EXPANSION, MODIFICATION, OR ADDITION TO THE LIMITATION AND EXCLUSION OF WARRANTIES IN THIS AGREEMENT.

CHIA USES AVAILABLE TECHNOLOGY TO MATCH PATIENT IDENTITIES WITH THEIR HEALTH INFORMATION IN ORDER TO PROVIDE PARTICIPANTS WITH DE-IDENTIFIED PATIENT INFORMATION. BECAUSE PATIENT INFORMATION IS MAINTAINED IN MULTIPLE PLACES, NOT ALL OF WHICH ARE ACCESSIBLE TO CHIA, AND BECAUSE NOT ALL PATIENT INFORMATION IS KEPT IN A STANDARD FASHION OR IS REGULARLY UPDATED, IT IS POSSIBLE THAT FALSE MATCHES MAY OCCUR OR THAT THERE MAY BE ERRORS OR OMISSIONS IN THE INFORMATION. CHIA DOES NOT AND CANNOT INDEPENDENTLY VERIFY OR REVIEW THE INFORMATION TRANSMITTED FOR ACCURACY OR COMPLETENESS.

Miscellaneous

1. Amendment of Agreement.

- i. A modification by a Party to this Agreement of its policies, procedures, processes, and/or systems used in connection with its obligations under this Agreement shall not be deemed a breach of or an amendment to this Agreement, unless (i) such modification unreasonably interferes with another Party's ability to fulfill its obligations under this Agreement, or (ii) such modification is contrary to or interferes with a specific obligation stated in the Application.
- ii. Any Party may seek to amend this Agreement in order to accommodate any new legislation, regulation, case holding, or legal order issued or proposed to be issued by a federal or state agency of competent jurisdiction, which, in the reasonable judgment of the party, (a) invalidates or is materially inconsistent with this Agreement; (b) would cause a Party to be in violation of the law by its continued performance under this Agreement; (c) would jeopardize the tax-exempt status of the Party (if applicable) by its continued performance under this Agreement; or (d) would jeopardize the licensure, accreditation, or participation in good standing in a federal health benefit plan of the Party by its continued performance under this Agreement. A Party wishing to seek such an amendment shall notify the other Parties in writing, including any proposed terms of amendment, no later than ninety (90) days prior to the proposed effective date of the amendment. The Parties shall then negotiate in good faith to agree upon an amendment. In the event no agreement is reached, no amendment shall be effective, and the Party seeking amendment may elect to terminate the Agreement by written notice.

2. Entire Agreement. This Agreement, including the Application and any attachments to the Application, incorporating this Agreement by reference, and as amended from time to time,

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

constitutes the entire agreement and understanding between the Parties and supersedes all prior oral or written agreements and understandings between them with respect to such services.

3. Assignment. No Party may assign or transfer any or all of its rights and/or obligations under this Agreement or any part of it, nor any benefit or interest in or under it, to any Third Party without the prior written consent of all other Parties.
4. Notices. Any notice that may be, or is required to be, given under this Agreement shall be written and shall be sent by first class mail, fax, courier, or as an Electronic Record attached to an e-mail. All notices shall be effective upon receipt at the addresses stated in the signature lines below.
5. Intent to Comply with Laws. This Agreement shall be interpreted consistently with all applicable information privacy and protection laws, and shall be construed and interpreted liberally in favor of the protection of protected health information and confidential information. In the event of a conflict between applicable laws, the more stringent law shall be applied.
6. Applicable Law for Judicial Proceedings. The laws of the Commonwealth of Massachusetts shall apply to all judicial proceedings arising out of this Agreement.
7. Mutual Representations.
 - i. Each party to this Agreement represents to the other Party that, at all times during the Term and at such other times as may be indicated, it shall comply with, and as applicable, shall require its directors, officers, and employees to comply with, its duties and obligations pursuant to this Agreement, including but not limited to duties and obligations that survive the termination of this Agreement.
8. Enforceability. If any provision of this Agreement is held invalid or unenforceable for any reason but would be valid and enforceable if appropriately modified, then such provision will apply with the modification necessary to make it valid and enforceable. If such provision cannot be so modified, the Parties agree that such invalidity will not affect the validity of the remaining provisions of the Agreement.
9. Force Majeure. Neither Party will be liable for nonperformance or delays caused by acts of God, wars, riots, strikes, fires, floods, earthquakes, government restrictions, terrorist acts, or other causes beyond its reasonable control.
10. Use of Electronic Signatures and Electronic Records. The Parties may elect to establish processes for the use of Electronic Records in the management of and compliance with this Agreement. Such document may include published policies, procedural information, notices, and any other document arising from or pertaining to this Agreement, including this Agreement itself. Any such process must include the establishment of a mutually acceptable Electronic Signature process, which complies with federal and state laws.

The undersigned further agrees to comply with the requirements set forth in M. G.L. c. 93H (data breaches), M.G.L. c. 93I (date destruction), 957 CMR 5.00 (CHIA data release), and any other applicable state or federal law or regulation applicable to the access, use, or disclosure of confidential or personal

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

data or protected health information. A Data Recipient who violates this Data Use Agreement, or 957 CMR 5.00, will be subject to all penalties and remedies allowed by law, including but not limited to M.G.L. c. 214 § 1B and M.G.L. c. 93A. CHIA will notify state and federal law enforcement officials, as applicable, of any violations of 957 CMR 5.00 and of any data breaches in connection with any violation of this agreement.

It is the sole responsibility of the Data Recipient to ensure compliance with all other local, state, and federal laws and regulations.

Signed:

Name of Data Recipient Organization

BY: _____
Authorized Signature

Name

Title

Date

Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)

Exhibit B – Data Use Agreement

**CENTER FOR HEALTH INFORMATION AND ANALYSIS
CONFIDENTIALITY AGREEMENT**

I, _____, hereby acknowledge that, in connection with a request for All-Payer Claims Database data and/or Hospital Discharge Database data under an agreement (the “Agreement”) with CHIA, I may acquire or have access to confidential information or individually identifiable information of patients. This information includes, but is not limited to, patient level protected health information (PHI - eligibility, claims, providers), health insurance coverage information, financial institution match information, as well as “personal data” as defined in G.L. c. 66A (collectively, the “Information”).

I will comply with all of the terms of the Agreement with CHIA regarding the access, use, and disclosure of any Information provided by CHIA.

I will at all times maintain the confidentiality of the Information. I will not inspect or “browse” the Information for any purpose not outlined in the Agreement. I will not access, or attempt to access, my own Information for any purpose. I will not access, or attempt to access, Information relating to any individual or entity with which I have a personal or financial relationship, for any reason. This includes family members, neighbors, relatives, friends, ex-spouses, their employers, or anyone not necessary for the work assigned. I will not, either directly or indirectly, disclose or otherwise make the Information available to any unauthorized person at any time.

I understand that any violations of this Agreement, M.G.L. c. 93H (regarding data breaches), M.G.L. c. 93I (regarding data destruction), and other laws protecting privacy and data security may subject me to criminal or civil liability. I further understand that CHIA will notify state and federal law enforcement officials, as applicable, of any data breaches in connection with any violation of this Agreement.

Signed:

Signature

Date

Print Name: _____

Title: _____

Organization: _____

Address: _____

Telephone: _____ E-Mail: _____

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

Exhibit C – Data Use Agreement

SAFEGUARDING CHIA DATA

I. Purpose

This document establishes confidentiality and security standards and procedures for all Data Recipients receiving CHIA Data that contain confidential data, personal data, or protected health information.

II. Definitions

For the purpose of this document, the term:

“Data Recipient” shall include any entity receiving CHIA Data pursuant to 957 CMR 5.04, 957 CMR 5.05, and/or 957 CMR 5.06.

“Employee” shall include all employees, contract employees, individual consultants, volunteers, trainees, student interns, members, directors, officers, partners, agents, and subcontractors who may have access to CHIA Data.

“CHIA Data” shall include any data received from CHIA pursuant to an approved request or application under 957 CMR 5.00.

“Media” shall include all forms of physical storage such as Compact Disks (CDs), DVDs, tapes, drives, and other storages devices.

III. General Requirements

The Data Recipient agrees that it will not use or further disclose CHIA Data other than as permitted or required by the Agreement.

The Data Recipient agrees to report to CHIA any unauthorized use or disclosure of CHIA Data of which it becomes aware within three (3) days of becoming aware of such unauthorized use or disclosure.

The Data Recipient must assign a Contract Manager, at a Director level or higher, to assume full responsibility for, and ensure compliance with, the Data Recipient’s data security standards and procedures.

When a Data Use Agreement expires or is terminated, all CHIA Data, files, and media in possession of the Data Recipient are to be destroyed consistent with the requirements of M.G.L. c. 93I or returned to CHIA. The Data Recipient must sign an affidavit, attached hereto as Exhibit D, confirming that all CHIA Data, files, and media have been returned to CHIA.

Access to areas containing the CHIA Data in any form (computer printout, photocopies, Media, notes, etc.) during the normal business day must be limited by creating restricted areas, security rooms, or locked rooms or files. Additionally, CHIA Data in any form (computer printout, photocopies, Media,

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

notes, etc.) must be protected during non-business hours by secured or locked premises, secured areas, or containerization.

The Data Recipient will implement rules and procedures to ensure that Employees do not leave computers or paper containing CHIA Data unprotected at any time.

CHIA Data must never be commingled with other Data Recipient information without CHIA's written authorization.

CHIA Data must never be transmitted or used on e-mail systems or sent via the Internet unless encrypted.

CHIA Data may not, under any circumstance, be removed from the Data Recipient's worksite(s).

The Data Recipient agrees to comply with state and federal laws applicable to CHIA Data, including Massachusetts data security regulations, 201 CMR 17.00, during the term of the Agreement.

IV. Safeguarding Hard-Copy CHIA Data

The Data Recipient will take all reasonable precautions to ensure the physical security of the CHIA Data under its control, including, but not limited to: fire protection; protection against smoke and water damage; alarm systems; locked files or rooms; limited access; or other means to prevent loss or unauthorized removal of data.

CHIA Data must never be in the open sight of any Employee not authorized to access CHIA Data.

CHIA Data must never be left unattended at an Employee's desk, the photocopy machine, the fax machine, or any common or accessible work spaces.

CHIA Data, and any material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers, if no longer needed, must be destroyed on site in manner compliant with M.G.L. c. 93I and any applicable federal requirements. Data destruction must be performed by individuals who have been authorized to have access to CHIA Data. CHIA Data must never be discarded whole, under any circumstance. The Data Recipient must maintain a log documenting the shredding of CHIA Data.

V. Safeguarding Electronic CHIA Data

The Data Recipient will continuously monitor the use of the CHIA Data maintained on its computer system to ensure that access to the data is limited to authorized Employees who have executed the Confidentiality Agreement attached as Exhibit B to the Data Use Agreement with CHIA.

The Data Recipient will require: passwords, access logs, badges, limited terminal access, limited access to input documents, design provisions to limit use of the CHIA Data, and any other reasonable means necessary to protect CHIA data from loss or unauthorized use or access. The Data Recipient must maintain data center access control logs.

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

The Data Recipient will ensure that Employees who are authorized to use the CHIA Data employ passwords that have certain parameters, including, but not limited to, at least eight characters, including at least one number, one symbol, and a mix of upper and lower case letters. Administrative passwords must be complex, must be maintained by the system administrator of the server, and must be unique to the functional area. No single password is to be maintained across all servers.

The Data Recipient will conduct periodic user account validation. The Data Recipient will immediately terminate access to the computer system of any person who is no longer authorized to access CHIA Data.

Any transmission of CHIA Data must occur over a secure and encrypted connection.

The Data Recipient's server system must be a dedicated system on an isolated network segment with current antivirus protection running at all times. The server system must be housed in a physically secure computer room with access controls.

CHIA Data may never be maintained on a mobile or portable device. This prohibition applies to laptop computers, Blackberries, smart phones, USB flash drives, Ipods, CD Roms, DVD's, floppy disks or the equivalent of any of these devices. Violation of this prohibition shall be grounds for immediate termination of the Data Use Agreement.

CHIA Data may be stored on hard disks if access control devices (hardware/software) have been installed and are receiving regularly scheduled maintenance, including upgrades. Access control should include password security, an audit trail, encryption or guided media, virus detection, and data overwriting capabilities.

Magnetic tape containing CHIA Data should be maintained in a separate pool of tapes and must not be made available for reuse or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape should be destroyed by cutting into lengths of 18 inches or less or by burning to effect complete incineration. All CHIA Data stored on magnetic media must be encrypted using either a software or hardware encryption methodology.

All access to the CHIA Data must be logged. The Data Recipient must house and maintain these logs. The Data Recipient will be required to provide CHIA with access to these logs upon request.

The Data Recipient may maintain the CHIA Data on its system only for as long as required for the project approved by CHIA.

VI. Vendors

The Data Recipient is not allowed to transfer CHIA Data to any third party, including contractors, vendors, or agents, without CHIA's written approval. All approved data transfers are subject to the same, or additional, conditions, as defined in the Data Use Agreement.

**Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)**

The Data Recipient shall provide CHIA with the names and contact information of all contractors, vendors, and agents who will be provided with access to CHIA Data. Prior to receiving access to CHIA Data, contractors, vendors, and agents must execute the Confidentiality Agreement attached to the Data Use Agreement as Exhibit B.

Center for Health Information and Analysis – Data Use Agreement – Non-Governmental
(Level 2 or Above)

Exhibit D – Data Use Agreement

CERTIFICATION OF PROJECT COMPLETION & DESTRUCTION OR RETENTION OF DATA

NOTE: CHIA Data must be destroyed so that it cannot be recovered from the electronic storage media. Acceptable methods include the use of file wiping software implementing at a minimum DoD.5200.28-STD (7) disk wiping, and the degaussing of backup tapes. Electronic storage media such as floppy disks, CDs, and DVDs used to store data must be made unusable by physical destruction. All data destruction must comply with the requirements of M.G.L. c. 93I.

The undersigned hereby certifies that the project described in this Application is complete as of this date: _____

The undersigned further certifies as follows (check the appropriate section):

I/we certify that we have destroyed all data received from CHIA in connection with this project, in all media that was used during the project. This includes, but is not limited to, data maintained on hard drives and other storage media.

I/we certify that we are retaining the data received in connection with the aforementioned project pursuant to the following health or research justification (please include an attachment providing detail and state how long the data will be retained).

I/we certify that we are retaining the data received from CHIA in connection with the aforementioned project as required by the following law:
[Reference the appropriate law and indicate the timeframe]

SIGNATURES:

Applicant: _____

Date: _____

For the Applicant's Organization: _____